Cybersecurity Tips for International Travel

1. Purpose
   The Best Practices workgroup was tasked with development of recommendations regarding international travel. The purpose of this document is to provide guidance for securing devices and data while traveling internationally on behalf of the State of Montana.

2. Policy
   Cybersecurity Tips for International Travel applies to the following controls found within the Information Security Policy.
   a. Information Security Policy
      - Identify
        - 1.8 – 1.8.9
      - Protect
        - 2.8 – 2.8.1, 2.9
   b. Information Security Policy – Appendix A
      - System and Information Integrity (SI)
        - SI-5 – Security Alerts, Advisories, and Directives
      - Program Management (PM)
        - PM-9 – Risk Management Strategy
        - PM-15 – Contacts with Security Groups and Associations
        - PM-16 – Threat Awareness Program
      - Awareness and Training (AT)
        - AT-2 – Security Awareness Training

3. Cybersecurity Tips for International Travel

   Personal privacy is not respected many nations. Unlike the United States, most other countries do not have legal restrictions against technical surveillance. State government employees are a potential high valued target for surveillance. Hotel rooms, meeting rooms, rental cars, taxis, and even commercial airlines may be subject to video and audio surveillance, along with other advanced monitoring techniques of electronic devices. Conversations may be monitored and local colleagues may be required to report conversations held with foreigners. Business and government travelers have reported their hotel rooms and belongings were searched while they were away. Sometimes there was no effort to conceal the search. Travelers should assume that all activity will be monitored and any information accessed may be exposed.

   The following tips have been compiled through various trusted sources in order to aid in awareness of threats and to counteract threat actors. Following these tips will reduce but not eliminate risk associated with the loss of confidentiality, integrity, and/or availability of State of Montana information and information systems along with personal loss of privacy.

   Prior to Departure

   - Identify electronic equipment needed – If the device is not essential, Do Not Take It!
     - If feasible, use a “clean” laptop, phone and new email account while traveling.

- Sanitize all devices. Cell phones can be hacked to steal contact lists, usernames, passwords, and browser history. Contact the helpdesk to aid in backing up and the subsequent purging/wiping of all data on the devices or substitute another piece of equipment that does not contain data.
- Remove apps requiring user accounts and passwords that are not necessary.
- Identify any data, internet access, or cloud access needed. Assume all information accessed while traveling will be compromised.
- Make an inventory of all devices that will be taken on the trip, including serial number, make, and model. Store it in a safe place with other key information (1 copy at home and 1 with you).
- Identify any accessories needed, cables, power adaptors and convertors. Accessories are routinely swapped for those with surveillance capabilities.
- Leave Bluetooth earpieces and keyboards at home and turn off devices' Bluetooth function, which can enable eavesdropping.
- Lock devices with a PIN or strong password (a combination of upper and lowercase letters, numbers and symbols at least 8 characters in length).
- Utilize whole disk encryption to protect stored data.
- Disable file sharing on computers.
- Patch, update and secure device (antivirus, antispyware, firewalls, encryption, VPN)
- Tape over or disable any integrated camera and disable integrated microphones.
- Review any guidelines or laws related to electronics for the country visiting and verify all web sites/cloud services needed can be accessed while traveling - http://travel.state.gov/content/passports/en/country.html.
- Create temporary accounts with strong passwords and do not use any of the passwords tied to current US accounts, including voice mail passwords.

- Obtain pre-travel country risk assessments for the country(s) from the State Department, and/or the FBI. There may be specific issues to be aware of and prepare for to ensure safety and peace of mind.
- Leave unneeded car keys, house keys, smart cards, credit cards, swipe cards, and access control devices at home.

During Travel

- Always carry electronics in carry-on luggage and keep in possession at all times.
- Keep devices in sight at all times and be aware of surroundings. Consider the use of a privacy screen to prevent shoulder surfing.
- Turn off geolocation services.
- Set email to retrieve manually and only download necessary email on trusted connections.
- Use a Virtual Private Network when on the Internet such as a secure wireless modem.
- Never use public Wi-Fi, cyber cafés, or other people's devices to access information electronically.
- Do not allow other people's electronic storage devices to connect to your device and do not connect to their devices.
- Do not use any USB drives given to you. They may be compromised.

- Do not post to social media.
- Accept that any information accessed will be exposed.
- Turn off devices when not in use.
- Respectfully but firmly decline to let customs officers take devices to another room to inspect them without you.
- Report any lost or stolen equipment immediately to the local US Embassy or Consulate and your IT staff.
- Beware of phishing or other social engineering attempts.

Upon Return

- Scan all data for viruses prior to copying it to another device.
- Wipe or format any electronic equipment immediately (treat as a compromised device).
- Consider destroying and replacing all SIM cards, depending on where you had traveled.
- Change all passwords used during travel and delete any temporary accounts used.
- Clear temporary internet files.
- Beware of any unexpected contacts from foreigners after your return.
- Report any unusual contact or circumstances to your IT security staff.

4. Compliance

   Compliance shall be evidenced by enterprise distribution of the Cyber Security Tips for International Travel as described above and personnel traveling internationally are made aware of the contents contained therein.

   Whereas, the Cybersecurity Tips for International Travel is not a policy document and compliance with its contents is not a requirement but is viewed as strongly recommended for personnel assigned to international travel on official State of Montana business. Moreover, awareness and adherence to its contents constitutes appropriate duty-of-care and expresses due diligence.

   Changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this Cybersecurity Tips for International Travel are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.